

Межсетевые экраны нового поколения Palo Alto Networks



the network security company™

Гольдштейн Андрей,
менеджер по развитию бизнеса продуктов ИБ

agold@netwell.ru, +7 (967) 285-85-68

Palo Alto Networks – общая информация

Общие сведения о компании

Основана в 2005 году; первая отгрузка в 2007

В России с 2010 года

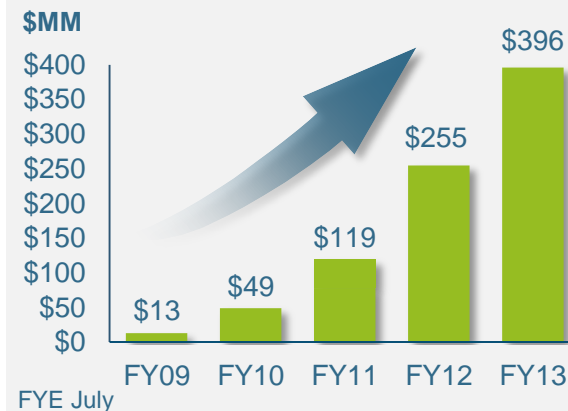
Офис и сервисный склад в г. Москва

Сертификация ФСТЭК по РД МЭ, НДС, 1 уровень защищенности персональных данных и гос. систем

269M\$ за первое полугодие 2014, 16000 клиентов

1,400+ сотрудников в мире

Оборот

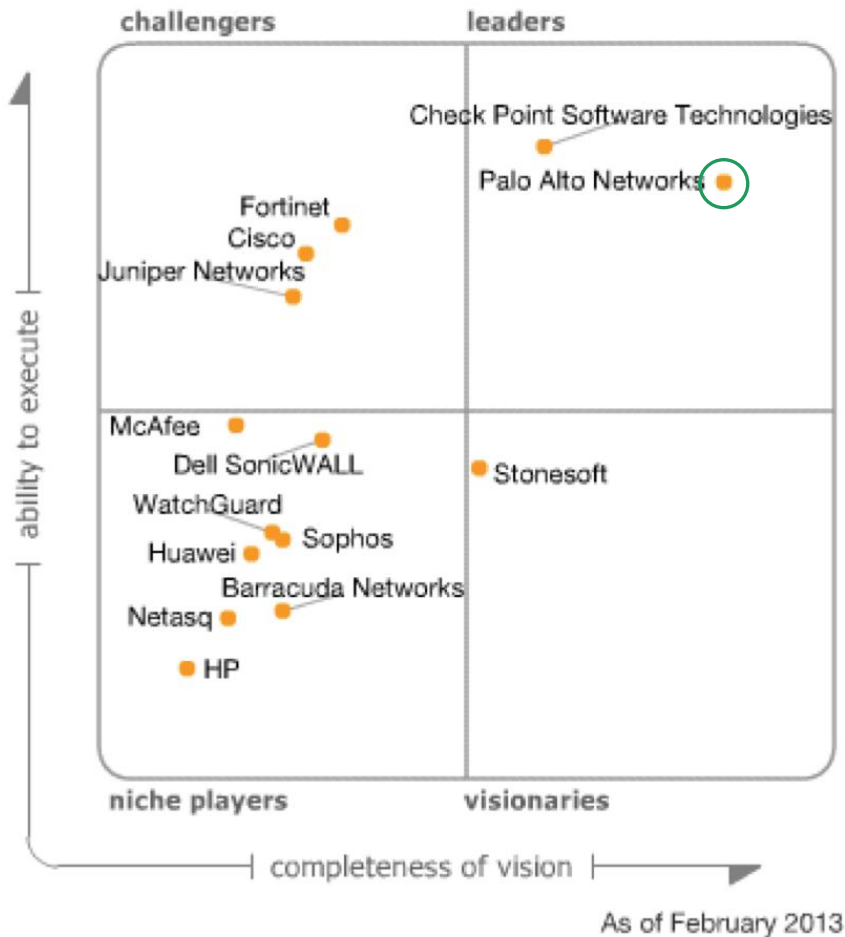


Количество заказчиков



Независимые тесты и рекомендации

2013 Magic Quadrant for Enterprise Network Firewalls



Решения Palo Alto Networks протестированы как NGFW и IPS и рекомендованы NSS Labs.

Source: Gartner (February 2013)

Ситуация в современных корпоративных сетях

Application Usage and Risk Report

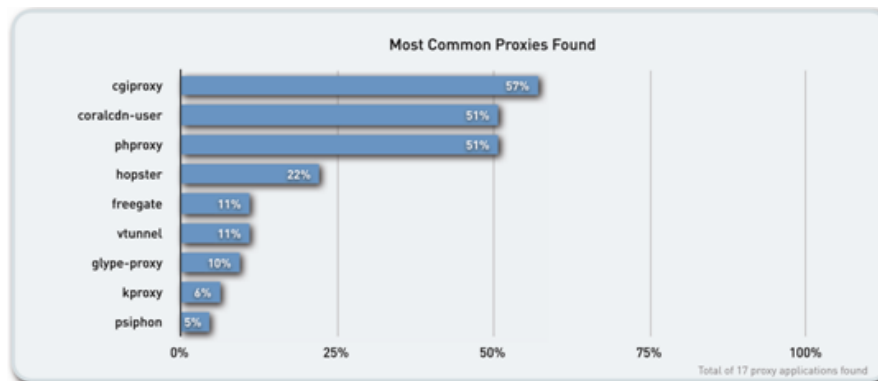
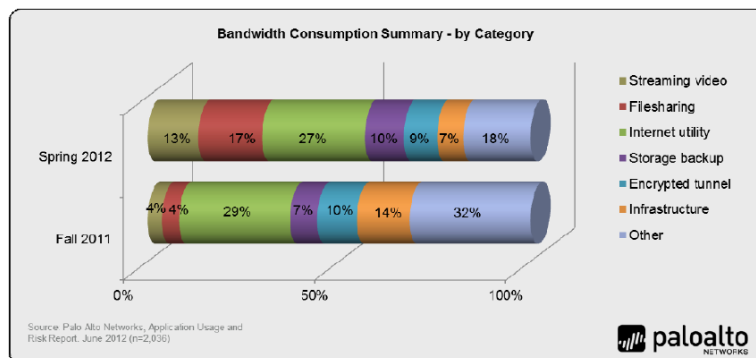
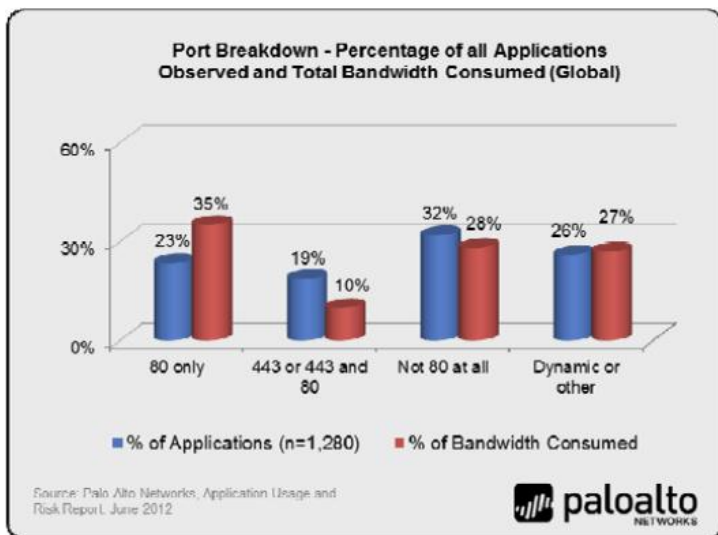


www.paloaltonetworks.com/aur

www.paloaltonetworks.com/app-usage-risk-report-visualization

Контроля приложений нет

- Анализ трафика 2000+ организаций: что происходит в современной сети?
 - 68% приложений (бизнес и пользовательских) для работы используют порты 80 и 443 или динамические порты, в т.ч. потоковое видео (13% пропускной способности)
 - Приложения, помогающие обойти политики безопасности, доступны каждому (бесплатные прокси – 81%, удаленный доступ к рабочему столу 95%, SSL туннели)
 - Очень широко распространены файл-обменные сети (P2P – 87%; браузерные)
 - 80+ социальных сетей (растет число, функциональность, нагрузка на сеть)



Риски использования таких приложений:
непрерывность бизнеса, потери данных,
продуктивность, финансовые затраты

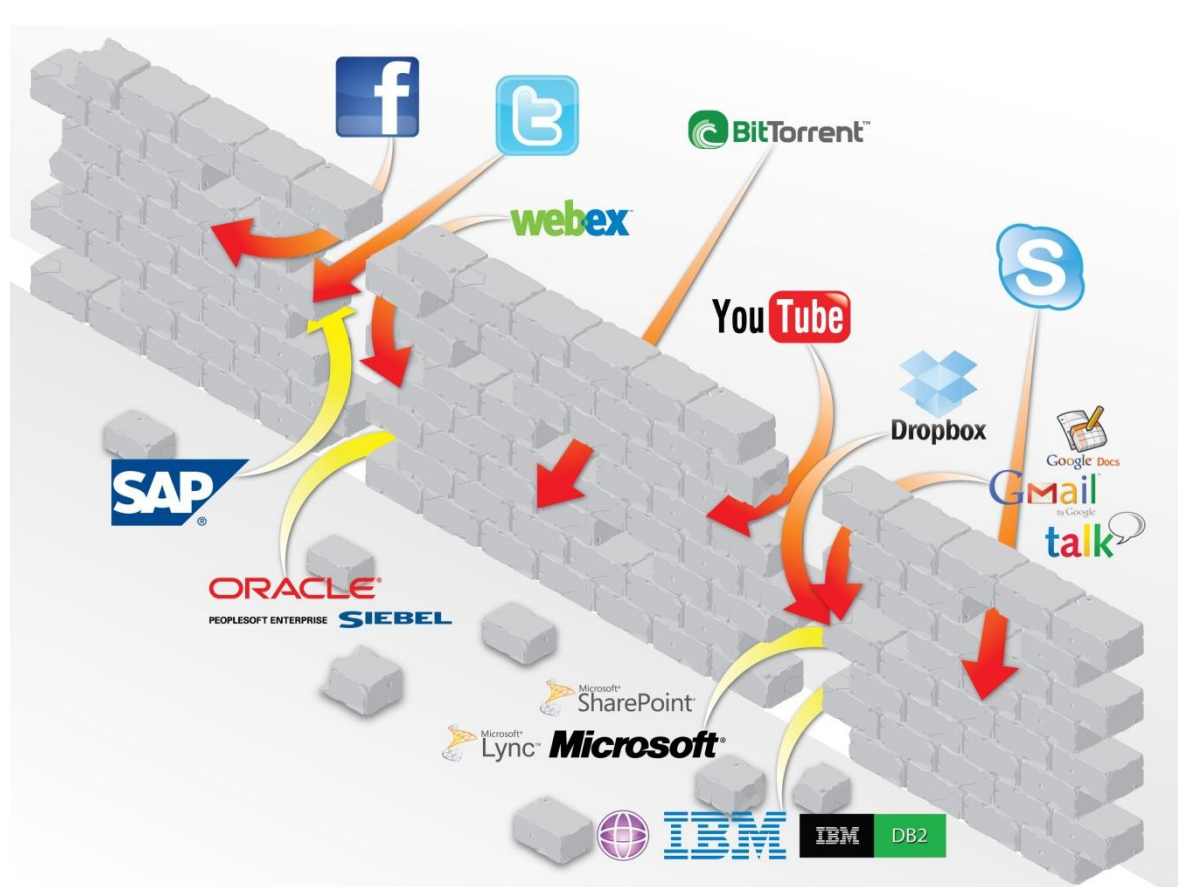
Проблемы межсетевого экранирования

Политики классических межсетевых экранов базируются на контроле:

- Портов
- IP-адресов
- Протоколов

НО...приложения изменились

- Порты \neq Приложения
- IP-адреса \neq Пользователи
- Протоколы \neq Контент



Межсетевой экран должен восстановить контроль над сетью

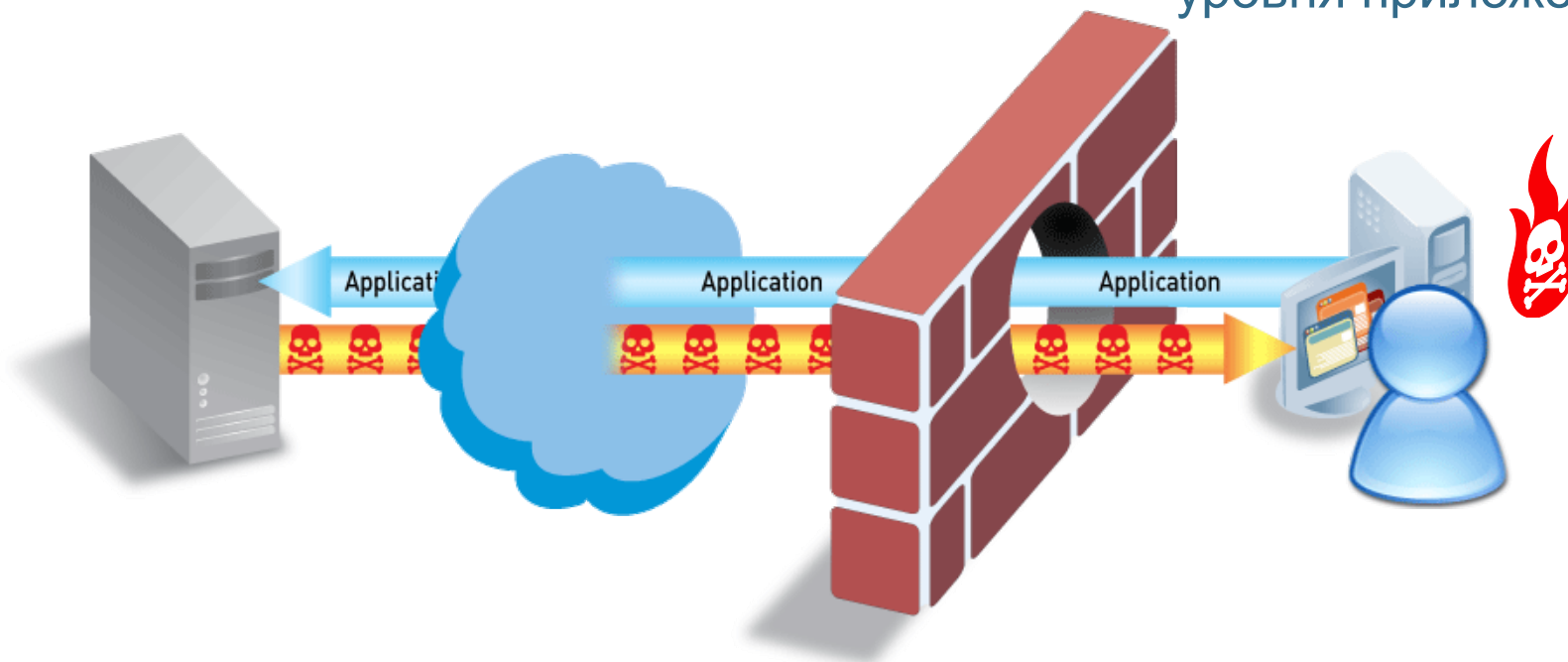
Приложения являются источником рисков

Приложения сами могут быть “угрозами”

- P2P file sharing, туннельные приложения, анонимайзеры, мультимедиа

Приложения могут способствовать распространению угроз

- Qualys Top 20 уязвимостей: основные угрозы – это угрозы уровня приложений

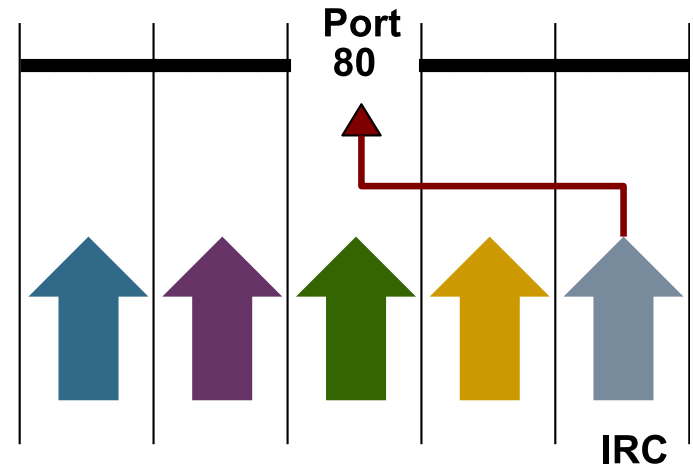


Приложения и угрозы уровня приложений создают бреши в системе безопасности

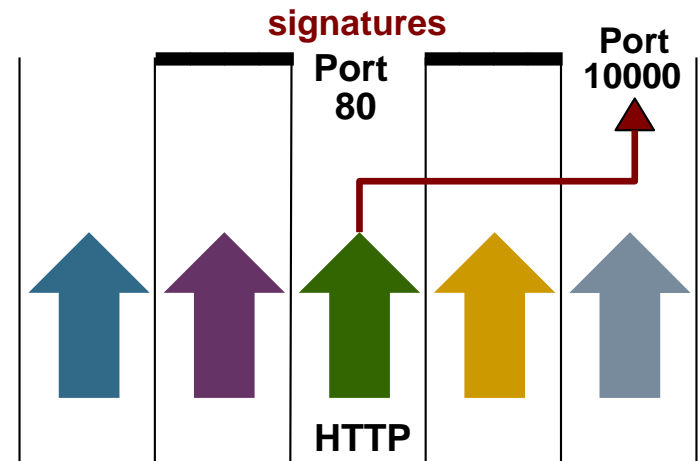
Техники уклонения от средств защиты

1. Распространение вредоносного ПО или нелегитимного трафика через открытые порты

- нестандартное использование стандартных портов
- создание новых специализированных протоколов для атаки



2. Использование стандартных протоколов на нестандартных портах – уклонение от сигнатурного сканирования



Использование туннелирования поверх DNS

Примеры

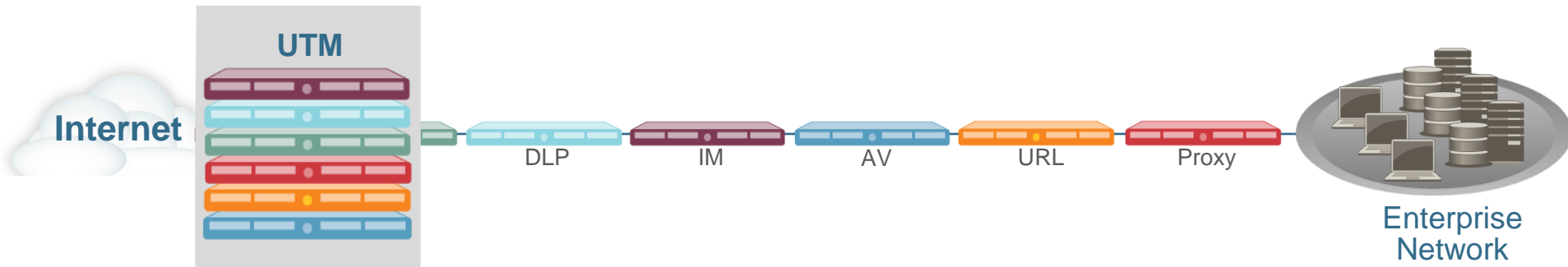
- tcp-over-dns
- dns2tcp
- Iodine
- Heyoka
- OzymanDNS
- NSTX

DNS	91 57916	53	Standard query TXT AAAAAAh5AA.=auth.ec2.mui
DNS	213 53	57916	Standard query response TXT
DNS	144 57916	53	Standard query TXT 2XKBgAABADFFNkQzMUNGOEE1
DNS	245 53	57916	Standard query response TXT
DNS	98 57916	53	Standard query TXT 2XI7KiF1AHNzaA.=connect.
DNS	199 53	57916	Standard query response TXT
DNS	85 57916	53	Standard query TXT 2XIAAAABBA.ec2.muides.co
DNS	240 53	57916	Standard query response TXT
DNS	85 57916	53	Standard query TXT 2XIAAQACBA.ec2.muides.co
DNS	113 57916	53	Standard query TXT 2XIAAADCFNTSC0yLjAtT3Bl
DNS	85 57916	53	Standard query TXT 2XIAAAAEBA.ec2.muides.co
DNS	253 57916	53	Standard query TXT 2XIAAAAFCAAAAXQIFPLjhQeS
DNS	85 57916	53	Standard query TXT 2XIAAAAGBA.ec2.muides.co


```
Authority RRs: 1
Additional RRs: 1
  ▸ Queries
  ▾ Answers
    ▾ AAAAAAh5AA.=auth.ec2.muides.com: type TXT, class IN
      Name: AAAAAAh5AA.=auth.ec2.muides.com
      Type: TXT (Text strings)
      Class: IN (0x0001)
      Time to live: 3 seconds
      Data length: 34
      Text: A2XIAAAh5ADA5VzNLWkdJNONLREwzREc
      text:
```

Использование рекурсивных запросов для передачи инкапсулированных сообщений по TCP в запросах удаленному DNS серверу и ответах клиенту

«Помощники» межсетевого экрана не помогают!



- Сложная топология и нет «прозрачной» интеграции
- «Помощники» межсетевого экрана не имеют полного представления о трафике – нет корреляции
- Дорогостоящее и дорогое в обслуживании решение
- Использование отдельных функциональных модулей в одном устройстве (UTM) делает его **ОЧЕНЬ** медленным

Межсетевой экран нового поколения

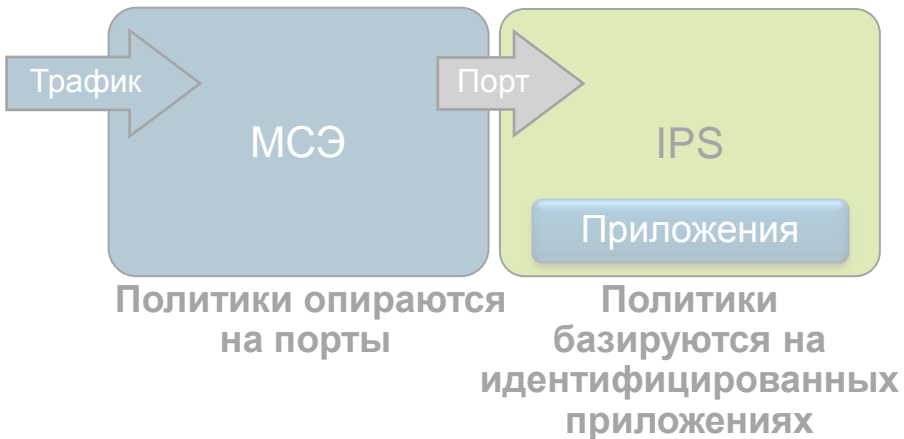
Пусть межсетевой экран делает свою работу!

Новые требования для межсетевого экрана:

1. Идентификация приложений
2. Идентификация пользователя
3. Защита против угроз
4. Многоуровневая детализация и контроль
5. Высокая производительность



Почему идентификация и контроль над приложениями должны быть на межсетевом экране



Контроль приложений Межсетевыми Экранами Нового Поколения

- Контроль над приложениями интегрирован в межсетевую экран = единая политика
- Идентификация приложений независимо от порта, постоянно и для всего трафика

Последствия

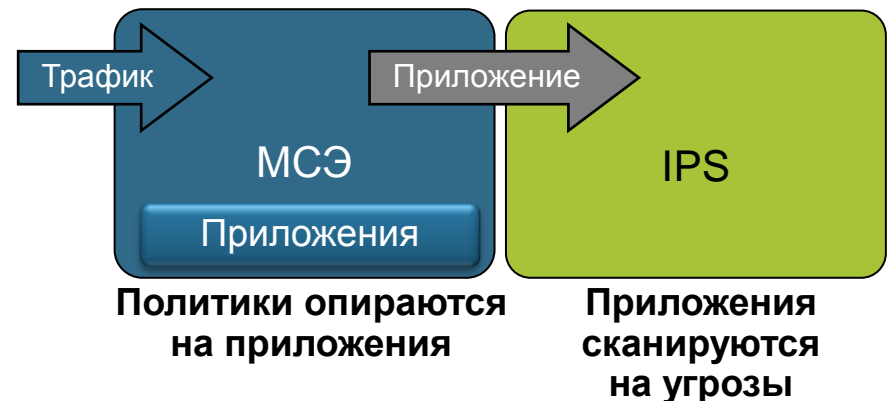
- Разрешение / запрет доступа к сети опираются на информацию о приложении
- Можно «безопасно разрешить» приложения

Контроль над приложениями как настройка

- Портовый МСЭ + Контроль приложений (IPS) = две политики
- Приложения как угрозы
 - Искать и блокировать только то, что задано в явном виде

Последствия

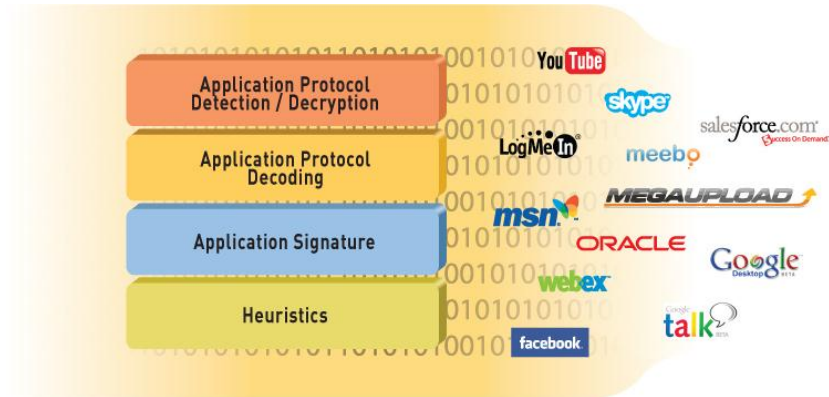
- Разрешение / запрет доступа к сети базируются на неполной информации
- Нельзя «безопасно разрешить» приложения
- Два хранилища некоррелируемых логов



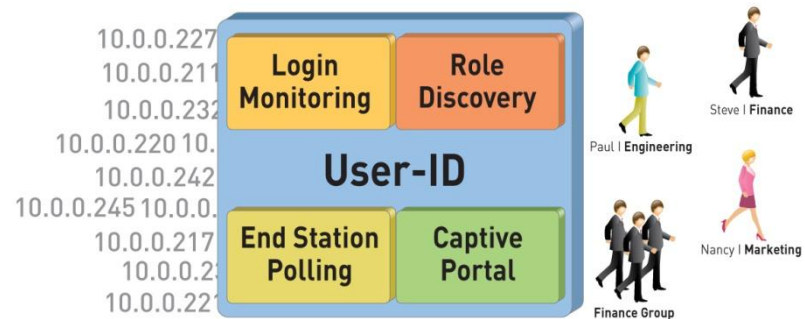
Технологии идентификации изменили межсетевой экран

FIREWALL

App-ID™
Идентификация приложений

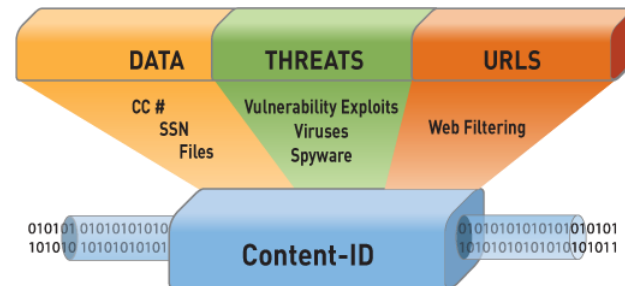


User-ID™
Идентификация пользователей

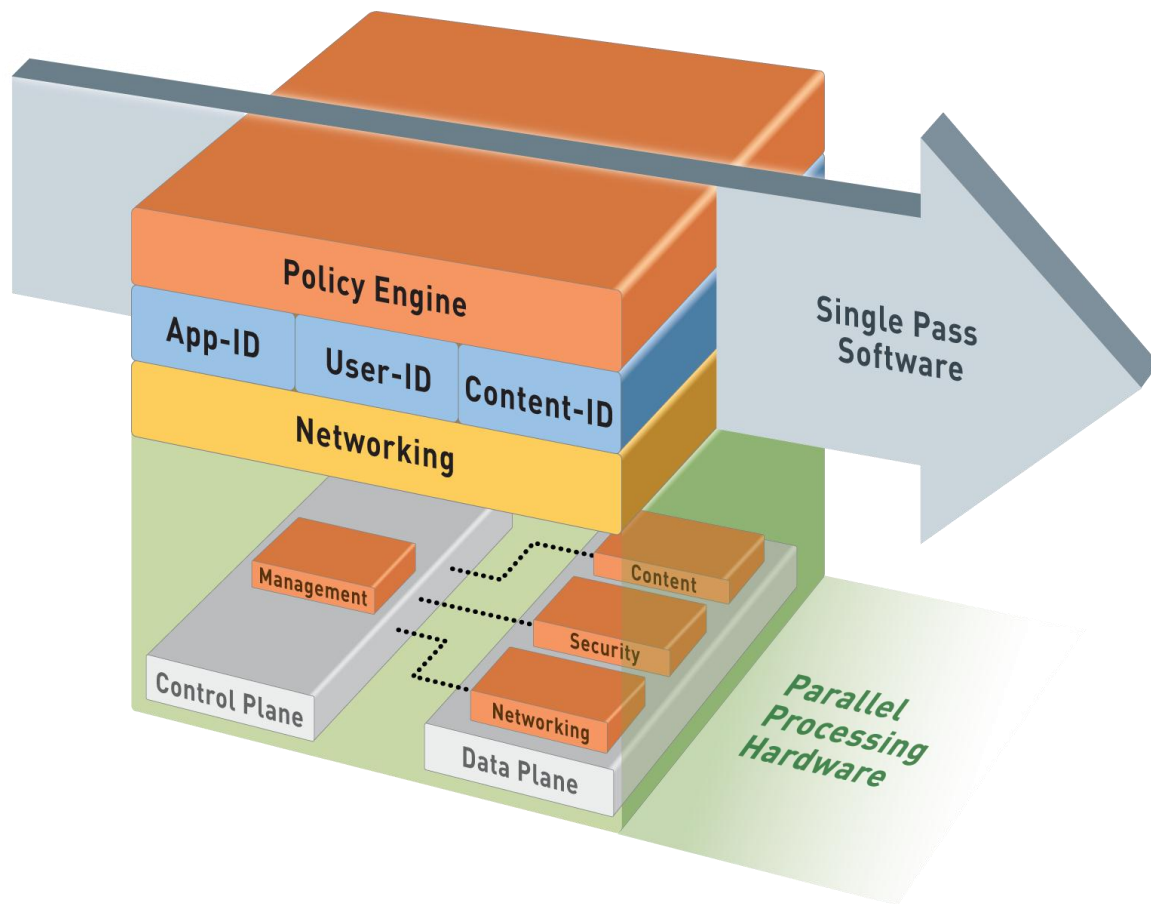


THREAT PREVENTION

Content-ID™
Контроль данных



Архитектура однопроходной параллельной обработки



Один проход

Каждый пакет сканируется только один раз

При сканировании одновременно определяется:

- Приложение
- Пользователь/группа
- Контент – угрозы, URL и т.д.

Параллельная обработка

Специализированное аппаратное обеспечение для каждой задачи

Разделение Data plane и Control plane

• До 120 Гбит/с, низкая задержка

Семейство платформ и функционал операционной системы

Семейство платформ Palo Alto Networks



PA-5060

- 20 Гбит/с FW/10 Гбит/с предотвращение атак/4,000,000 сессий
- 4 SFP+ (10 Gig), 8 SFP (1 Gig), 12 RJ-45 gigabit



PA-5050

- 10 Гбит/с FW/5 Гбит/с предотвращение атак /2,000,000 сессий
- 4 SFP+ (10 Gig), 8 SFP (1 Gig), 12 RJ-45 gigabit



PA-5020

- 5 Гбит/с FW/2 Гбит/с предотвращение атак /1,000,000 сессий
- 8 SFP, 12 RJ-45 gigabit



PA-3050

- 4 Гбит/с FW
- 2 Гбит/с предотвращение атак
- 500,000 сессий
- 12 copper gigabit
- 8 SFP interfaces



PA-3020

- 2 Гбит/с FW
- 1 Гбит/с предотвращение атак
- 250,000 сессий
- 12 copper gigabit
- 8 SFP interfaces



VM Series (VMware/Citrix SDX)

- до 1 Гбит/с FW
- До 600 Мбит/с предотвращение атак
- до 250,000 сессий
- Гостевая машина или в режиме гипервизора



PA-2050

- 1 Гбит/с FW/500 Мбит/с предотвращение атак/250,000 сессий
- 4 SFP, 16 RJ-45 gigabit



PA-2020

- 500 Мбит/с FW/200 Мбит/с предотвращение атак /125,000 сессий
- 2 SFP, 12 RJ-45 gigabit



PA-500

- 250 Мбит/с FW/100 Мбит/с предотвращение атак /64,000 сессий
- 8 copper gigabit



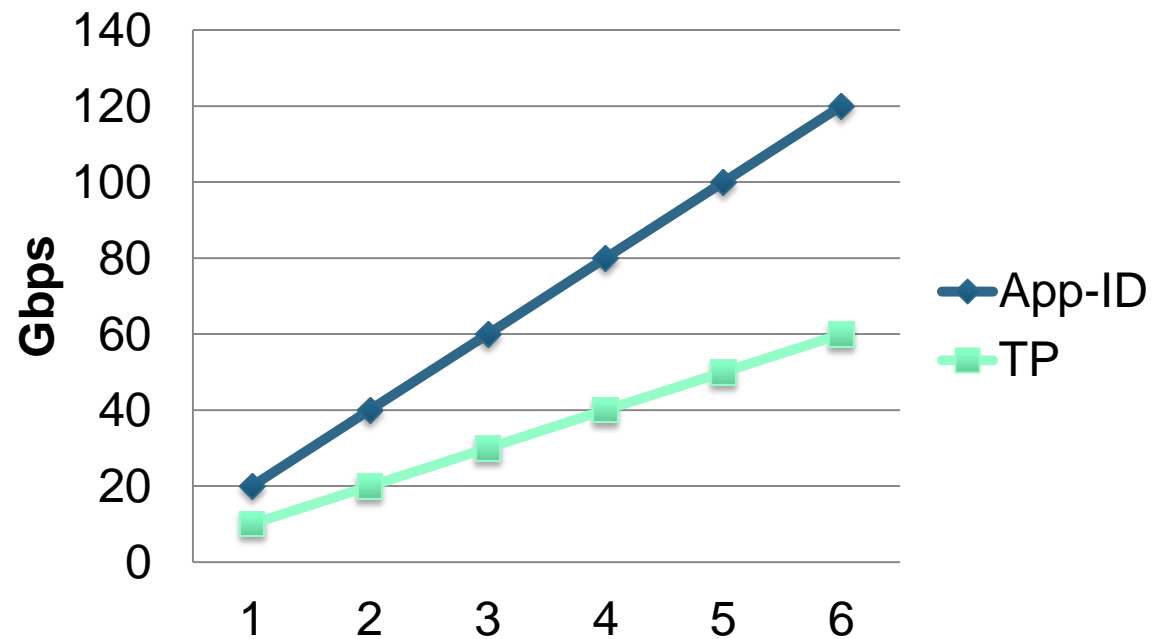
PA-200

- 100 Мбит/с FW/50 Мбит/с предотвращение атак/64,000 сессий
- 4 copper gigabit

PA-7050 - самый производительный в мире NGFW



	PA-7050 NPC	PA-7050 System
FW + App Control Gbps	20	120
Threat Prev. (IPS+AV) Gbps	10+	60+



Основной функционал операционной системы

Идентификация и контроль приложений, пользователей и контента дополняются следующим функционалом

• Network

- Динамическая маршрутизация (BGP, OSPF, RIPv2)
- Режим мониторинга – подключение к SPAN-порту
- Прозрачный (L1) / L2 / L3 режимы
- Маршрутизация по политикам (PBF)
- IPv6

• VPN

- Site-to-site IPsec VPN
- SSL VPN (GlobalProtect)

• Функционал QoS

- Приоритезация, обеспечение максимальной/гарантированной полосы
- Возможна привязка к пользователям, приложениям, интерфейсам, зонам и т.д.
- Мониторинг полосы в режиме реального времени

• Зоновый подход

- Все интерфейсы включаются в зоны безопасности для упрощения настройки политик

• Отказоустойчивость

- Active/active, active/passive
- Синхронизация конфигурации
- Синхронизация сессий (кроме PA-200, VM-series)
- Path, link и HA мониторинг

• Виртуальные системы

- Настройка нескольких межсетевых экранов в одном устройстве (для серии PA-2000 и выше)

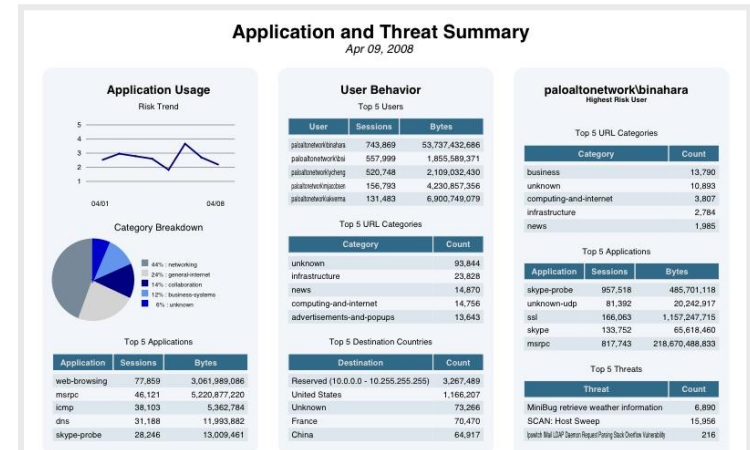
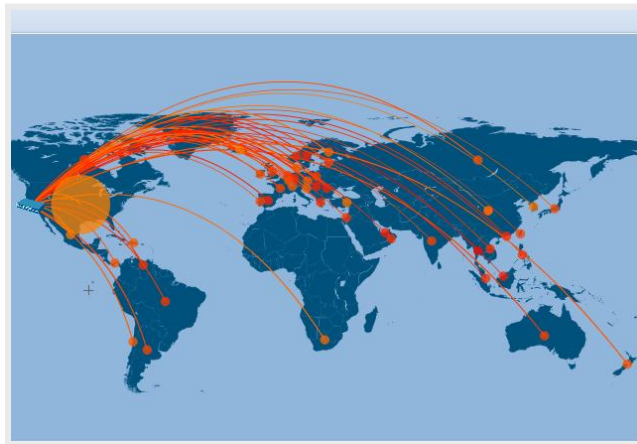
• Простое и гибкое управление

- CLI, Web, Panorama, SNMP, Syslog, NetFlow, интеграция с SIEM/SIM

Управление

Средства управления, отчетности и интеграции

- Web GUI, SSH, XML API
- Централизованное управление – ПО Panorama + M-100
- Богатая отчетность из коробки
- Отправка логов по Syslog, SNMP
- Интеграция с SEIM/SIM (например, HP ArcSight, Symantec SIM)



Category	Subcategory	Technology	Risk	Characteristic
116 business-systems	9 auth-service	41 browser-based	179 1	107 Vulnerabilities
129 collaboration	13 database	129 client-server	63 2	55 Prone to Misuse
73 general-internet	11 encrypted-tunnel	150 network-protocol	49 3	159 Widely used
49 media	7 erp-crm	4 peer-to-peer	17 4	20 Excessive Bandwidth
218 networking	19 general-business		26 5	103 Transfers Files
2 unknown	23 infrastructure			53 Evasive
	116 ip-protocol			46 Used by Malware
	37 management			61 Tunnels Other Apps

Name	Shared	Category	Subcategory	Risk	Technology
3pc	✓	networking	ip-protocol	1	network-protocol
active-directory	✓	business-systems	auth-service	2	client-server
activenet	✓	networking	ip-protocol	1	network-protocol
afp	✓	business-systems	storage-backup	3	client-server
altris	✓	business-systems	management	1	client-server
apc-powerchute	✓	business-systems	general-business	2	client-server
apple-airport	✓	networking	infrastructure	2	network-protocol
apple-update	✓	business-systems	software-update	3	client-server
argus	✓	networking	ip-protocol	1	network-protocol
aris	✓	networking	ip-protocol	1	network-protocol
asproxy	✓	networking	proxy	3	browser-based
avamar	✓	business-systems	storage-backup	2	client-server
avaya-phone-ping	✓	business-systems	management	2	client-server
avocent	✓	networking	remote-access	3	client-server
avoidr	✓	networking	proxy	3	browser-based
backweb-exec	✓	business-systems	storage-backup	3	client-server
backweb	✓	business-systems	erp-crm	1	browser-based
bbn-rcv-mon	✓	networking	ip-protocol	1	network-protocol
beinsync	✓	networking	remote-access	2	client-server

Trends

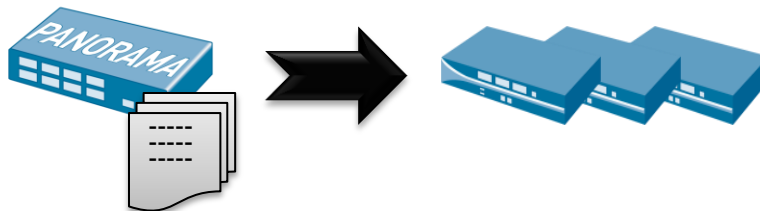
Bandwidth

Threats

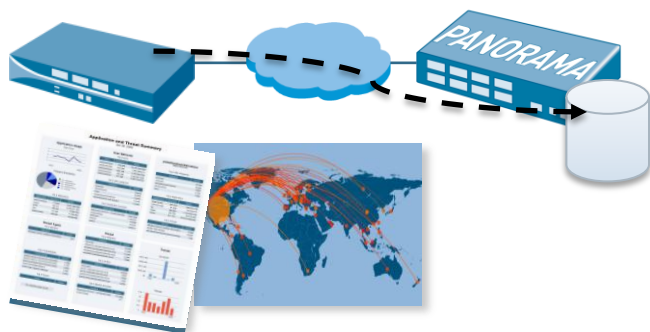
0401 0408

Централизованное управление с использованием ПО Panorama

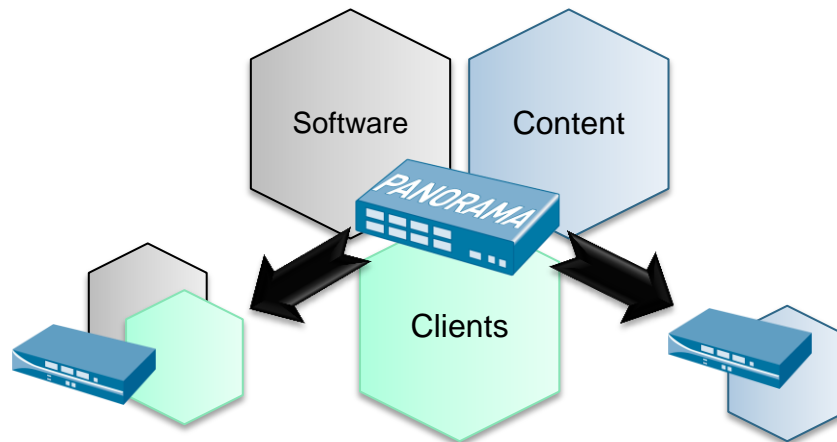
- Централизованная настройка



- Централизованное логирование и отчетность



- Централизованное обновление



- Ролевое администрирование



**VM-series – межсетевой экран
нового поколения для защиты
среды виртуализации VMware**

VM-series: назначение и реализация

VM-series – межсетевой экран нового поколения, который обеспечивает применение технологий Palo Alto Networks в среде виртуализации, включая:

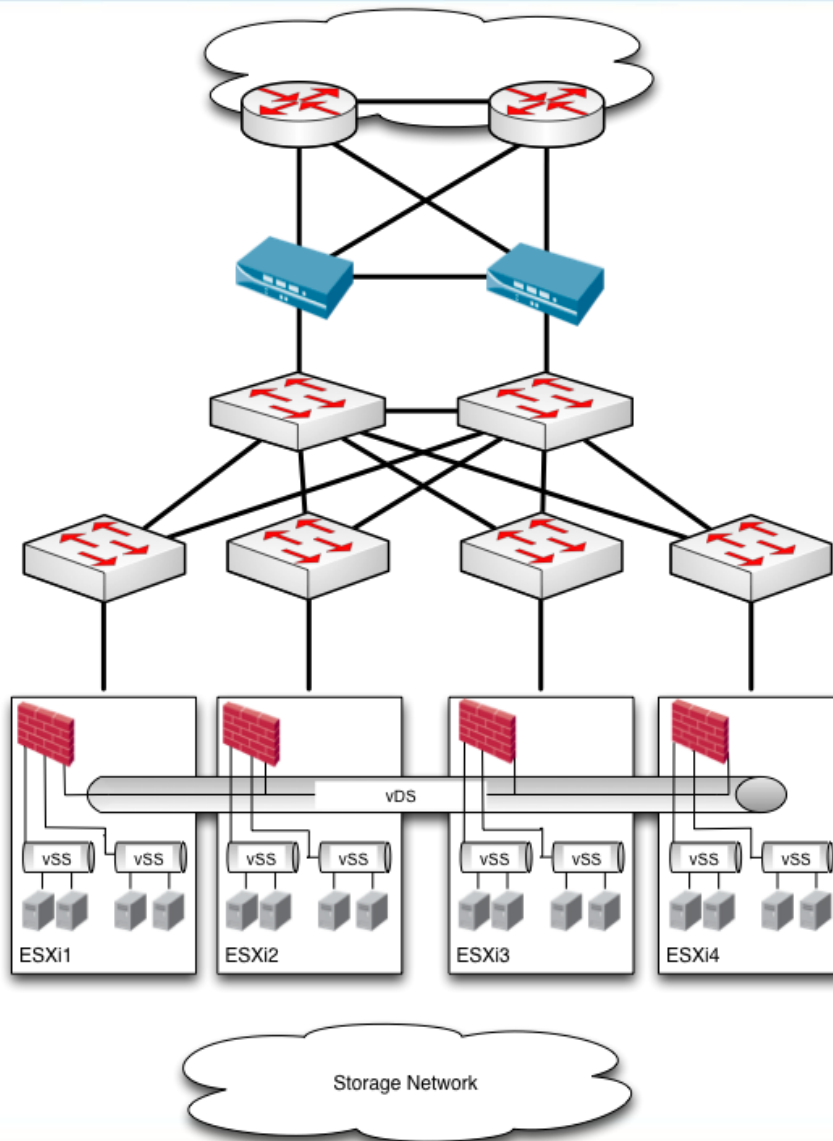
- App-ID
- User-ID
- Content-ID (IPS, AV/AS, WildFire, URL-фильтрацию, блокировку файлов)

Это ключевое отличие Palo Alto Networks VM-series от виртуальных портовых МЭ, таких как vShield.

VM-series реализован как гостевая виртуальная машина (VMware virtual appliance), исполняемая гипервизором ESXi и подключаемая к защищаемым сегментам сети (PGs, VLANs), организованным на базе виртуальных коммутаторов vSwitch/Nexus 1000v.

VM-series обеспечивает контроль, инспекцию и визуализацию трафика между виртуальными машинами.

Архитектура виртуализированного ЦОД



Software Stack

Security Management

Network Management

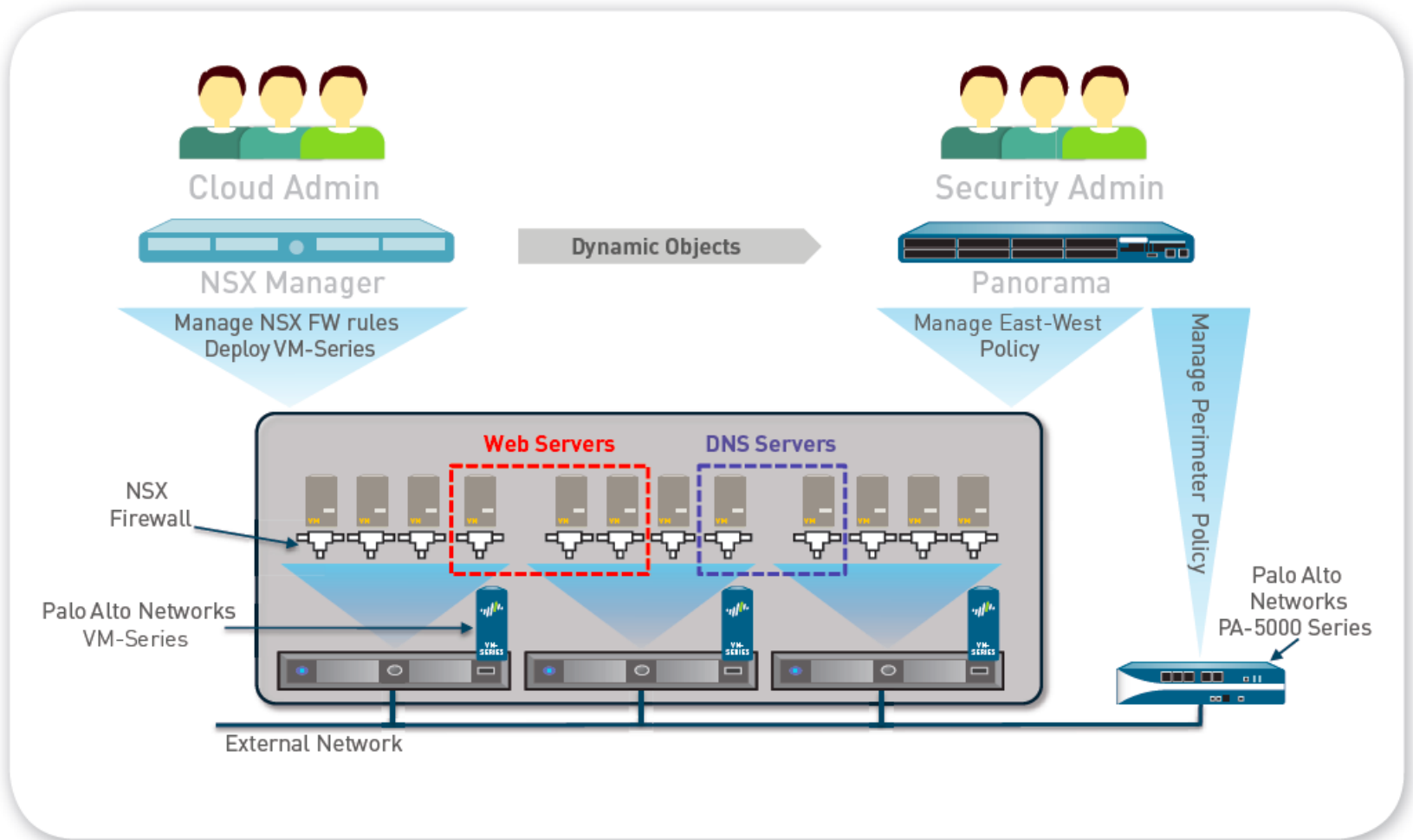
Systems Management

Storage Management

•Virtualization Management

•Orchestration

VM-Series VMware NSX Edition – режим гипервизора



WildFire – облачный сервис обнаружения вредоносного ПО «нулевого дня»

Ключевые этапы современной сетевой атаки



1

Приманка

Завлечь использовать специальное ПО, открыть файл или перейти на веб-сайт с вредоносами

2

Эксплоит

Зараженный контент использует уязвимости установленного ПО без ведома пользователя

3

Загрузка ПО для «черного хода»

В фоне загружается и устанавливается второй вредонос

4

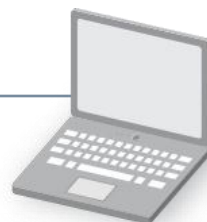
Установление обратного канала

Вредонос устанавливает исходящее подключение для связи с злоумышленником

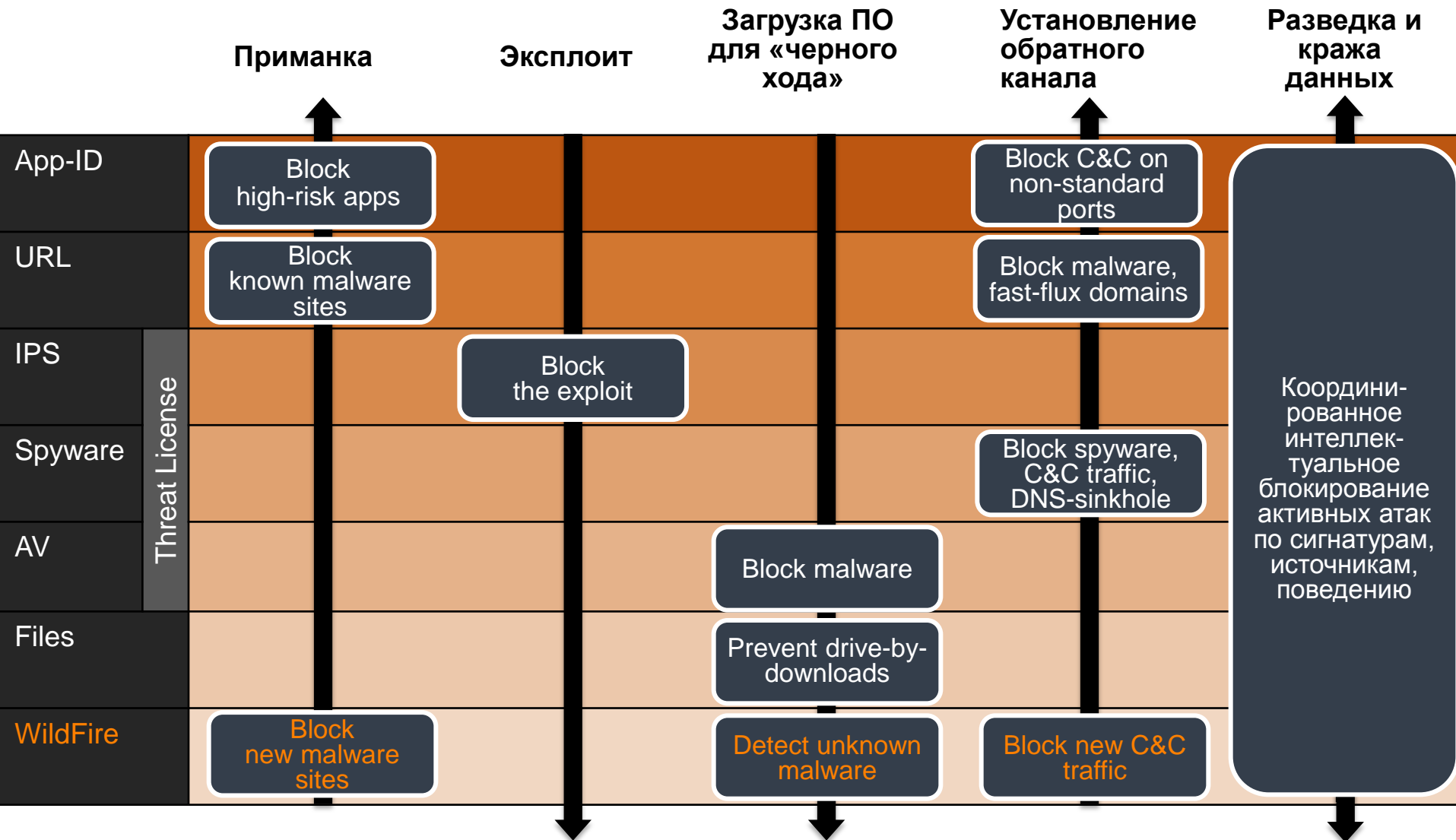
5

Разведка и кража данных

Удаленный злоумышленник имеет доступ внутри сети и проводит атаку



Система защиты следующего поколения от целенаправленных атак и угроз «нулевого» дня



Как работает сервис WildFire

Автоматическая или по запросу генерация сигнатуры в «облаке»



Изолированная сеть



Анализируется 100+ типов поведения

40% новых экземпляров – это вариации одних и тех же вредоносных

Сигнатура автоматически создается и загружается на все устройства в течение 30 минут

1 сигнатура покрывает до 1500+ уникальных хэшей SHA

WF-500 проверяет до 4500 **уникальных** файлов в день: исполняемые, офисные, PDF

IN THE PAST

7

DAYS

3760

NEW MALWARE
FILES FOUND

W I L D F I R E

1824

MALWARE NOT DETECTED BY
TOP AV PRODUCTS


48%

PERCENTAGE OF
UNDETECTED MALWARE

Dashboard
Reports Upload File


Today

Wildfire Stats



■ Malware
■ Benign
■ Pending

Wildfire Stats



■ Malware
■ Benign
■ Pending

Device	Malware	Benign	Pending	Registered
0003C101538	1	5	0	10/27/2011 01:50:12
0003C103099	11	19	0	10/31/2011 04:46:21
0004A100237	5	15	0	11/03/2011 09:10:01
0008C106977	0	2	0	11/07/2011 02:13:27
0006C106979	10	0	0	11/03/2011 03:23:12

Reports
Dashboard Upload File

Search

Source

Type

Search

Showing 26 to 50 | [first](#) | [prev](#) | [next](#)

Received Time	Source	Filename	URL	Verdict
11/07/2011 11:47 AM	0004A100237	Vimeo.dll	update.videoraptor.com/8.0_slideshow/Vimeo.dll	Benign
11/07/2011 11:40 AM	0004A100237	k3000patch11.05.exe	unknown	Benign
11/07/2011 11:38 AM	0004A100237	k3000patch11.05.exe	unknown	Benign
11/07/2011 10:54 AM	0003C101538	f5u109_xp.exe	cache-www.belkin.com/support/dl/f5u109_xp.exe	Benign
11/07/2011 10:48 AM	0004A100237	WeatherSetup.exe	toolbar.inbox.com/dnl/toolbar/80474/WeatherSetup.exe	Benign
11/07/2011 09:54 AM	0003C101538	Spider90.ocx	qc.ctsnp.local/qcbin/Spider90.ocx	Benign
11/07/2011 09:54 AM	0003C101538	Spider90.ocx	qc.ctsnp.local/qcbin/Spider90.ocx	Benign
11/07/2011 09:53 AM	0004A100237	Google.AdMob.Ads.WindowsPhone7.dll	apps-p.marketplace.windowsphone.com/740AEDF1-3861-4EBA-ABF2-E6D	Benign
11/07/2011 09:52 AM	0004A100237	CleverSoftware.Phone.Translate.dll	apps-p.marketplace.windowsphone.com/740AEDF1-3861-4EBA-ABF2-E6D	Benign
11/07/2011 09:50 AM	0003C101538	Add_Area_Iteration_Nodes.exe	blogs.microsoft.co.il/files/folders/219449/download.aspx	Benign
11/07/2011 09:50 AM	0003C101538	Add_Area_Iteration_Nodes.exe	blogs.microsoft.co.il/files/folders/219449/download.aspx	Benign
11/07/2011 09:41 AM	0003C103099	.exe	unknown	Malware
11/07/2011 08:39 AM	0004A100237	wpsetup.exe	audiochannel.net/components/wpsetup.exe	Benign

Пример детального отчета о вредоносном файле



Общая информация

Имя файла, hash, URL, source & destination, вердикт (вредонос или нет), приложение

Filename:	transcript.scr		
SHA256:	4f325b6b63cf7c0daf8ca3ed72a182f05c6fe2d19f1991bce45723697571ad61		
URL:	unknown		
User:	unknown	Received:	11/4/2011 9:06:49 PM
Source:	133.5.184.202 :110	Destination:	133.6.215.213 :39887
Hostname/Mgmt. IP:	PA-2050	Application:	pop3
Verdict:	Malware	Virus Coverage Information	Покрытие AV

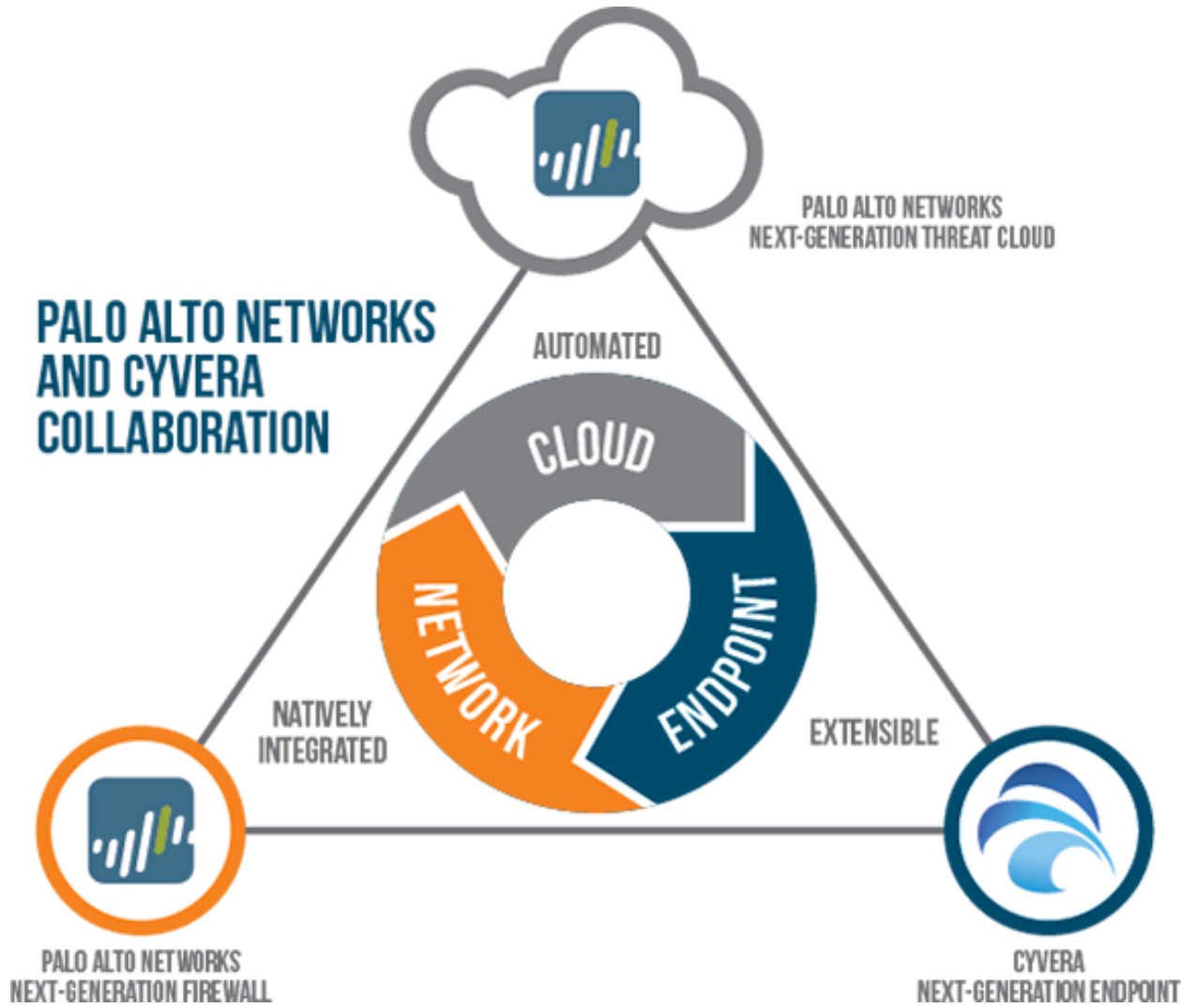
Результаты анализа поведения

Список подозрительных действий, выполненных файлом в «песочнице»

Created an executable file in Windows folder
Stole saved user passwords from Internet Explorer
Created or modified files
Spawned new processes
Masqueraded as a Windows system program
Modified Windows registries
Modified registries or system configuration to enable auto start capability
Accessed honey files
Changed security settings of Internet Explorer
Changed the proxy settings for Internet Explorer
Modified the network connections setting for Internet Explorer
Sent out emails

Анализ 100+ видов поведения. Одни безвредны сами по себе, другие используются только вредоносными.

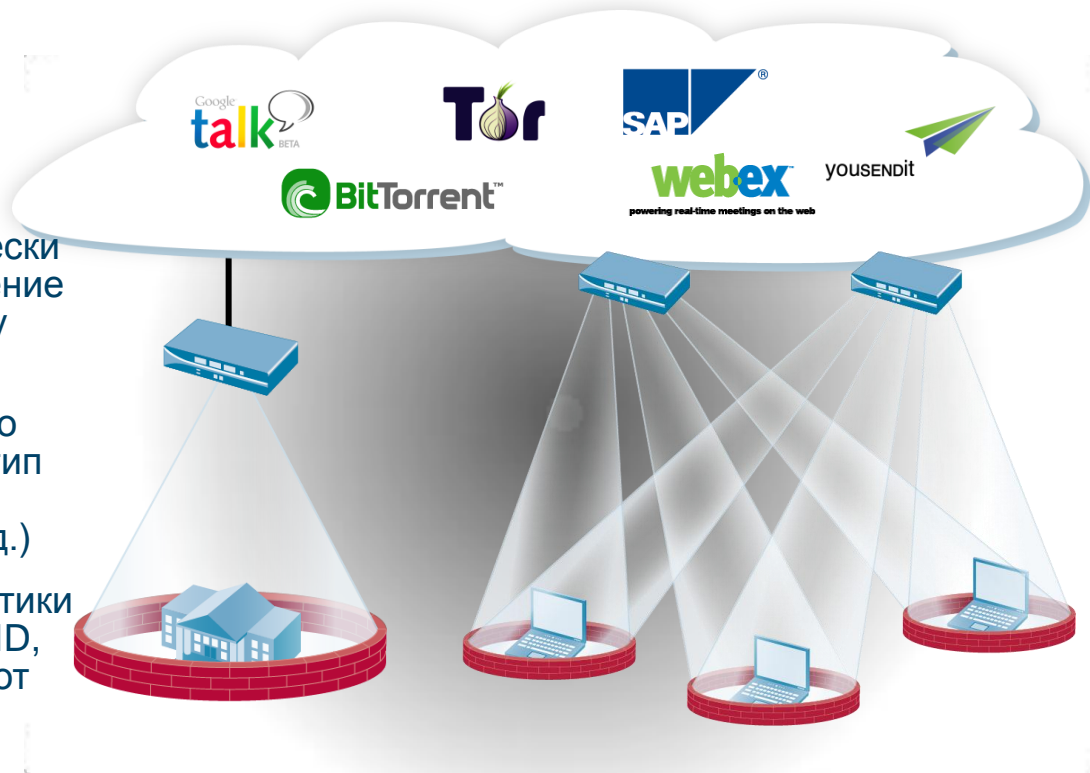
Дальнейшее развитие защиты от угроз нулевого дня



**Global Protect –
безопасное подключение по SSL/IPsec
VPN мобильных пользователей
и удаленных офисов**

Функционал GlobalProtect

- Пользователи никогда не работают “off-network” независимо от их местоположения
- Межсетевые экраны образуют «облако» сетевой безопасности
- Как это работает:
 - Программный агент определяет местоположение клиента (внутри корпоративной сети или нет)
 - Если клиент находится вне корпоративной сети, то автоматически устанавливается SSL VPN соединение к ближайшему межсетевому экрану
 - Агент также может предоставлять межсетевому экрану информацию о состоянии безопасности клиента (тип клиента, установленные патчи, шифрование диска, антивирус и т.д.)
 - Межсетевой экран применяет политики безопасности, основанные на App-ID, User-ID, Content-ID и информации от агента



Доступны клиенты GlobalProtect для настольных и мобильных ОС

- Windows, Mac OS X
- Для Apple iOS в App Store
- Для Android в Google Play
- Автоматическое или ручное подключение

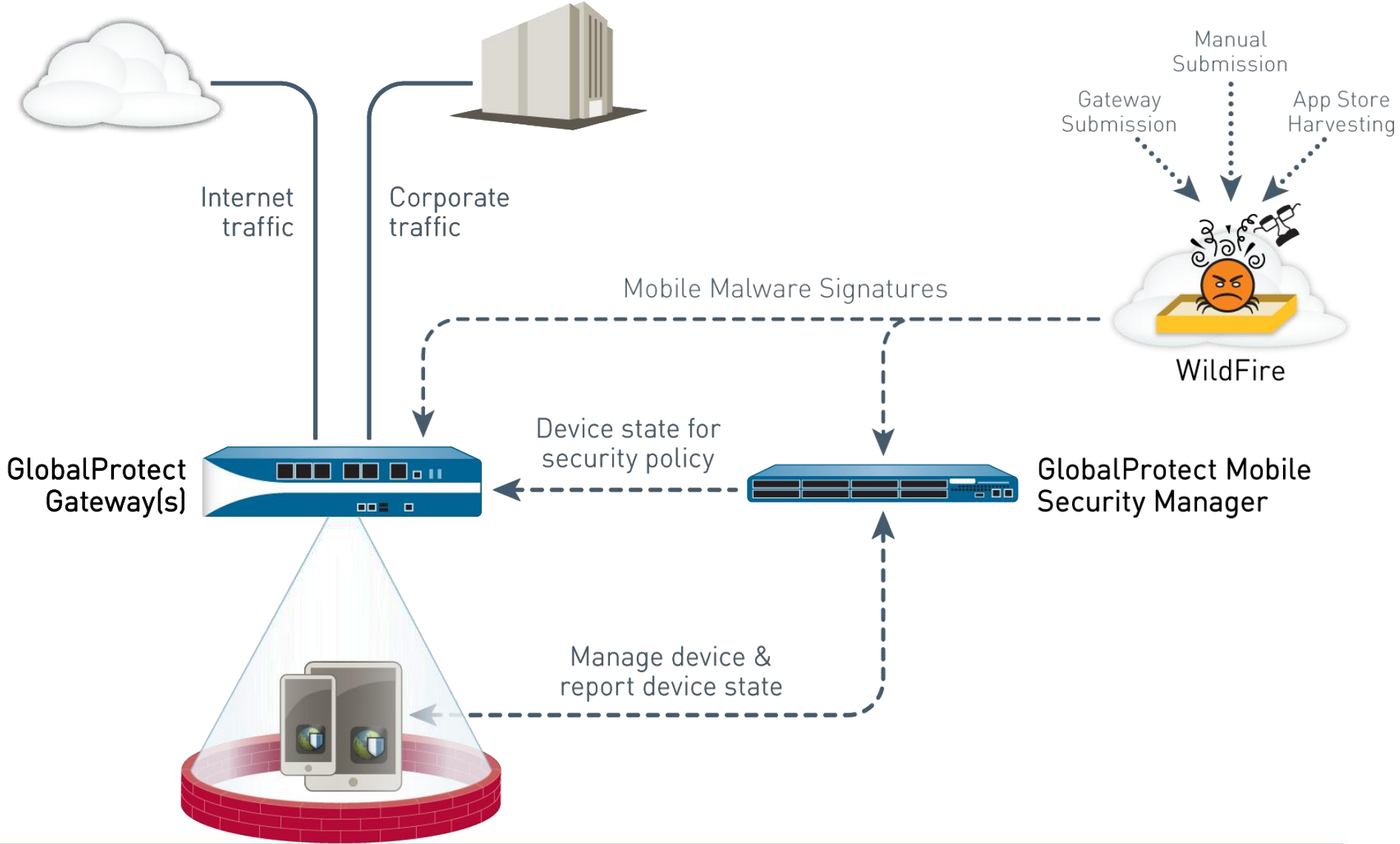


The screenshot shows the GlobalProtect mobile application interface. At the top, the status bar displays 'AT&T LTE VPN', the time '9:20 AM', and '100%' battery. Below the status bar are two tabs: 'Info' (selected) and 'Details'. The main content area is a table with the following data:

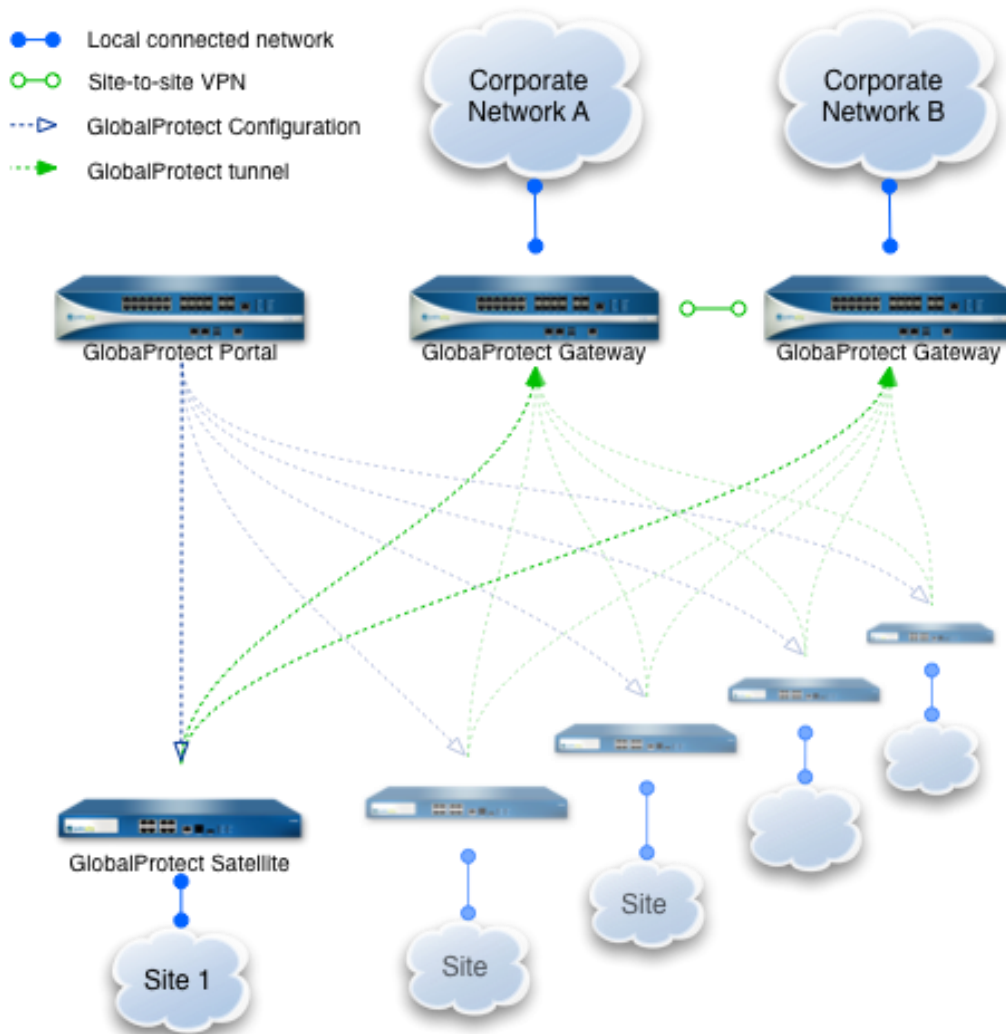
Status	Connected
Network	Cellular
Gateway	Denver GW gw34.paloaltonetworks.com
Local Address	10.244.31.32
Gateway Address	192.168.38.1
Protocol	IPSec
Bytes In/Out	11.6MB / 487.7KB
Packets In/Out	10361 / 6244
Error Packets In/Out	0 / 0

At the bottom of the screen is a navigation bar with four icons: 'Home' (house icon), 'Status' (shield icon), 'Messages' (envelope icon with a red notification bubble containing the number '1'), and 'Help' (question mark icon).

GlobalProtect Mobile Security Manager



Легкое развертывание Large Scale VPN с GlobalProtect



1 GP Portal в HQ/DC

Несколько GP Gateways в HQ/DCs

Сотни/тысячи GP Satellites в филиалах и мини-офисах с простой настройкой – достаточно только подключения к Интернет/WAN



the network security company™